

(11)Publication number : 11-003284

(43) Date of publication of application : 06.01.1999

(51)Int.Cl.

G06F 12/14

G06K 17/00

G06K 19/07

(21)Application number : 09-152687

(71)Applicant : MITSUBISHI ELECTRIC CORP

(22)Date of filing : 10.06.1997

(72)Inventor : KORIN MEESON

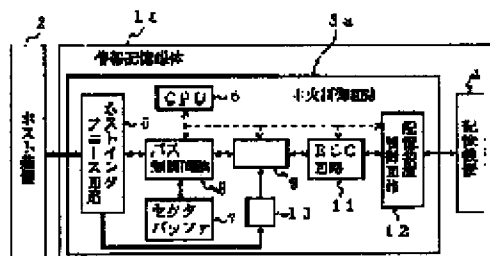
SHINOHARA TAKAYUKI

(54) INFORMATION STORAGE MEDIUM AND ITS SECURITY METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To ensue the security function while keeping high versatility for an information storage medium by ciphering selectively the data received from a host device and decoding the stored data.

SOLUTION: When a host device 2 writes the new file data into an information storage medium 1a, a central controller 3a identifies whether the written data are the file management data or the file data based on the logical address value that is designated by the device 2.



If the file management data are identified, a ciphering/decoding circuit 9 is not started and accordingly the data are not processed and stored in a storage 4 as they are. If the file data are identified, the circuit 9 is started to perform a ciphering operation based on the key information set by a ciphering/decoding key setting circuit 10. Then the ciphered data are written into a prescribed address of the storage 4 via a storage control circuit 12. This operation is reversed when the file data are read out of the medium 1a.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-3284

(43) 公開日 平成11年(1999) 1月6日

(51) Int.Cl.⁸

識別記号

F I

G 0 6 F 12/14

3 2 0

G 0 6 F 12/14

3 2 0 B

G 0 6 K 17/00

G 0 6 K 17/00

E

19/07

19/00

N

審査請求 未請求 請求項の数10 O L (全 7 頁)

(21) 出願番号 特願平9-152687

(22) 出願日 平成9年(1997) 6月10日

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 コリン・メーソン

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(72) 発明者 篠原 隆幸

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

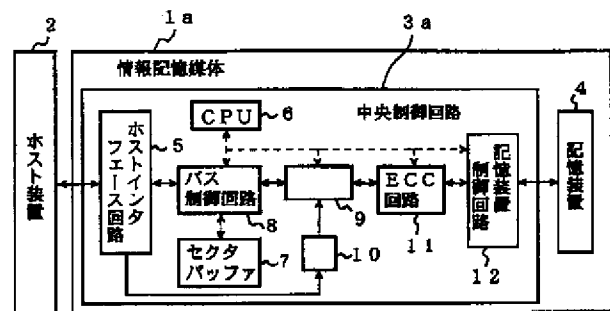
(74) 代理人 弁理士 田澤 博昭 (外1名)

(54) 【発明の名称】 情報記憶媒体およびそのセキュリティ方法

(57) 【要約】

【課題】 情報記憶媒体に格納される貴重な個人情報とその汎用性故に容易に他人に読まれてしまうという課題があった。

【解決手段】 暗号化・復号化回路が機密性の高い個人情報であるファイルデータに対してのみ暗号化を実行し、既知であるファイル管理用のデータは平文のまま記憶装置に書き込みするように情報記憶媒体のセキュリティシステムを構築したので、この暗号方式で第三者による解読を困難にし高いセキュリティ機能が実現できる。



6 : CPU (中央処理装置)

9 : 暗号化・復号化回路 (演算回路、第1演算回路)

10 : 暗号化・復号化キー設定回路 (演算回路、第2演算回路)

【特許請求の範囲】

【請求項 1】 中央処理装置と、ホスト装置とデータ交換するインタフェース回路と、データを格納する記憶装置と、ホスト装置からのデータを選択的に暗号化し格納されたデータを復号化する演算回路とを備えた情報記憶媒体。

【請求項 2】 演算回路はホスト装置からのデータをファイル単位で選択的に暗号化することを特徴とする請求項 1 記載の情報記憶媒体。

【請求項 3】 ホスト装置からのコマンドに応じて演算回路を有効または無効にする選択手段を更に備えたことを特徴とする請求項 1 または請求項 2 記載の情報記憶媒体。

【請求項 4】 中央処理装置と、ホスト装置とデータ交換するインタフェース回路と、データを格納する記憶装置と、必要時にデータの書き込み・読み出し双方時にそれぞれ暗号化・復号化する第 1 演算回路と、任意的にデータの書き込み・読み出しの双方時にそれぞれ暗号化・復号化する第 2 演算回路とを備えた情報記憶媒体。

【請求項 5】 第 2 演算回路で行われる暗号化・復号化処理はその回路が更新またはリセットされるまで有効であることを特徴とする請求項 4 記載の情報記憶媒体。

【請求項 6】 セクタデータ領域に書き込まれるデータを暗号化し、ファイル管理データに書き込まれるデータには暗号化しない情報記憶媒体のセキュリティ方法。

【請求項 7】 ホスト装置からのコマンドに応じて書き込みデータに暗号化・復号化を実行することを特徴とする請求項 6 記載の情報記憶媒体のセキュリティ方法。

【請求項 8】 書き込みデータには通常の暗号化・復号化を実行し、特殊キーデータの入力時には他の暗号化・復号化を実行する情報記憶媒体のセキュリティ方法。

【請求項 9】 特殊キーデータの入力ホスト装置からのコマンドまたは情報記憶媒体に直接行われることを特徴とする請求項 8 記載の情報記憶媒体のセキュリティ方法。

【請求項 10】 特殊キーデータの入力ホスト装置からのコマンドまたは装置リセットないし電源オフまで有効であることを特徴とする請求項 9 記載の情報記憶媒体のセキュリティ方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、情報処理装置の外部記憶媒体として使用される、フラッシュメモリ、EEPROM、磁気ディスクメモリ等の記憶装置を搭載した情報記憶媒体およびそのセキュリティ方法に関するものである。

【0002】

【従来の技術】 電池による駆動を前提として携帯型情報端末機器の外部記憶媒体として、ICカード、中でもフラッシュATAPCカード（以下、PCカードと略称す

る）等の情報記憶媒体の普及が進んでいる。図 7 は、従来のフラッシュATAPCカード等の情報記憶媒体の機能ブロック図であり、図において、1e は情報記憶媒体、2 はホスト装置、3e は中央制御回路、4 はフラッシュメモリ、EEPROM、磁気ディスクメモリ等の記憶装置、5 はホストインタフェース回路、6 はマイクロプロセッサ（MPU）等の中央処理装置（CPU）、7 はセクタバッファ、8 はバス制御回路、11 は誤り訂正コードすなわち ECC（Error Correction Code）回路、12 は記憶装置制御回路である。

【0003】 中央制御回路 3e は、ホストインタフェース回路 5、CPU 6、セクタバッファ 7、バス制御回路 8、ECC 回路 11、記憶装置制御回路 12 から構成され、これらを 1 つの集積回路 IC チップに搭載することができる。また、ECC 回路 11 はわずかなビットの誤りならば検出のみでなくその訂正も行う機能を有する。

【0004】 次に動作について説明する。この情報記憶媒体 1e へのデータの書き込みについては、ホスト装置 2 が情報記憶媒体 1e に新たなファイルデータを書き込む場合、ホスト装置 2 上の DOS はファイル名、サイズ、作成日時等の情報からなるディレクトリ情報と、そのファイルデータの論理的な格納場所を示す FAT（File Allocation Table）情報を所定の論理アドレスに書き込んだ後、ファイルデータをデータ領域に書き込む。このとき、中央制御回路 3e は、ホストインタフェース回路 5 を介して一時的にセクタバッファ 7 に蓄えられたデータをホスト装置 2 が指定する論理アドレス値に応じて平文のまま記憶装置 4 の所定の領域（ヘッダ領域、セクタデータ領域、ECC 領域）に書き込まれる。

【0005】 データの読み出しであるが、これはホスト装置 2 とホストインタフェース回路 5 を介して CPU 6 が通信して記憶装置 4 から格納データをセクタバッファ 7 を介して順次読み出していく。この際、格納データは平文のままなのでデータ変換操作は伴わない。

【0006】

【発明が解決しようとする課題】 従来の PC カード等の情報記憶媒体は以上のように構成されているので、ハードディスク用のドライバソフトウェアによる読み書きが可能な汎用性の高い記憶媒体であるが、それゆえに情報記憶媒体 1e 内に格納される貴重な個人情報も容易に他人に読まれてしまうという課題があった。この対策として、情報記憶媒体 1e に格納される全ての情報に対して暗号化を実行し、セキュリティ機能を持たせることなどが考えられるが、このような暗号化機能を付加した情報記憶媒体 1e のアクセスには専用のドライバソフトウェアが必須となり、その汎用性が損なわれてしまう。

【0007】 この発明は上記のような課題を解決するためになされたもので、PC カード等の情報記憶媒体とし

ての汎用性の高さを保ちつつ、ユーザが他人に読まれたくないデータ（ファイル）のみを選択的に暗号化してフラッシュメモリ等の記憶装置に格納可能なセキュリティ機能付きの情報記憶媒体を得ることを目的とする。

【0008】

【課題を解決するための手段】請求項1記載の発明に係る情報記憶媒体は、中央処理装置と、ホスト装置とデータ交換するインタフェース回路と、データを格納する記憶装置と、ホスト装置からのデータを選択的に暗号化し格納されたデータを復号化する演算回路とを備えたものである。

【0009】請求項2記載の発明に係る情報記憶媒体は、演算回路はホスト装置からのデータをファイル単位で選択的に暗号化するものである。

【0010】請求項3記載の発明に係る情報記憶媒体は、ホスト装置からのコマンドに応じて演算回路を有効または無効にする選択手段を更に備えたものである。

【0011】請求項4記載の発明に係る情報記憶媒体は、中央処理装置と、ホスト装置とデータ交換するインタフェース回路と、データを格納する記憶装置と、必要20的にデータの書き込み・読み出し双方時にそれぞれ暗号化・復号化する第1演算回路と、任意的にデータの書き込み・読み出しの双方時にそれぞれ暗号化・復号化する第2演算回路とを備えたものである。

【0012】請求項5記載の発明に係る情報記憶媒体は、第2演算回路で行われる暗号化・復号化処理はその回路が更新またはリセットされるまで有効とするものである。

【0013】請求項6記載の発明に係る情報記憶媒体のセキュリティ方法は、セクタデータ領域に書き込まれるデータを暗号化し、ファイル管理データに書き込まれるデータには暗号化しないものである。

【0014】請求項7記載の発明に係る情報記憶媒体のセキュリティ方法は、ホスト装置からのコマンドに応じて書き込みデータに暗号化・復号化を実行するものである。

【0015】請求項8記載の発明に係る情報記憶媒体のセキュリティ方法は、書き込みデータには通常の暗号化・復号化を実行し、特殊キーデータの入力時には他の暗号化・復号化を実行するものである。

【0016】請求項9記載の発明に係る情報記憶媒体のセキュリティ方法は、特殊キーデータの入力がホスト装置からのコマンドまたは情報記憶媒体に直接行われるものである。

【0017】請求項10記載の発明に係る情報記憶媒体のセキュリティ方法は、特殊キーデータの入力が新たなキーデータ入力時または装置リセットないし電源オフまで有効とするものである。

【0018】

【発明の実施の形態】以下、この発明の実施の一形態を

説明する。

実施の形態1. 図1は、この発明の実施の形態1によるフラッシュATAPCカード等の情報記憶媒体の機能ブロック図であり、図において、1aは情報記憶媒体、2はホスト装置、3aは中央制御回路、4はフラッシュメモリ、EEPROM、磁気ディスクメモリ等の記憶装置、5はホストインタフェース回路、6はマイクロプロセッサ(MPU)等のCPU(中央処理装置)、7はセクタバッファ、8はバス制御回路、9は暗号化・復号化回路(演算回路、第1演算回路)、10は暗号化・復号化キー設定回路(演算回路、第2演算回路)、11は誤り訂正コードすなわちECC回路、12は記憶装置制御回路である。

【0019】中央制御回路3aは、ホストインタフェース回路5、CPU6、セクタバッファ7、バス制御回路8、暗号化・復号化回路9、暗号化・復号化キー設定回路10、ECC回路11、記憶装置制御回路12から構成され、これらを1つの集積回路ICチップに搭載することができる。

【0020】図2は、一般的なディスクオペレーティングシステム(DOS)でフォーマットされたPCカード等の情報記憶媒体1内部のデータ構造図である。このようにDOSはその容量に応じて情報記憶媒体1のパーティショニング情報、ブート情報、およびファイル管理用の情報(FATおよびディレクトリエントリ)を規定の領域に書き込むことによりフォーマットを実行する。これらの情報のうち、ファイル管理用の情報(FAT (File Allocation Table)およびディレクトリエントリ)は、ファイルデータの書き込みの都度その内容が更新される。

【0021】さらに図3は、情報記憶媒体1のフラッシュメモリ等の記憶装置4に格納されるセクタデータの構成を示した図である。ヘッダ領域には一般的にそのセクタデータに付された論理セクタ番号が書き込まれ、読み出し時にID情報として参照される。セクタデータ領域には書き込むべきユーザデータが格納され、ヘッダ情報およびセクタデータに対するECC(Error Correction Code)データがECC領域に格納される。

40 【0022】次に動作について説明する。まず、データの書き込みについて説明する。図1において、ホスト装置2が情報記憶媒体1aへ新たなファイルデータを書き込む場合、ホスト装置2上のDOSには、ファイル名、サイズ、作成日時等の情報からなるディレクトリエントリ情報と、そのファイルデータの論理的な格納場所を示すFAT(File Allocation Table)情報を所定の論理アドレスに書き込まれた後に、ファイルデータがデータ領域に書き込まれる。

【0023】このとき、中央制御回路3aでは、ホスト装置2により指定された論理アドレス値に基づいて、書

き込みデータがファイル管理用データかファイルデータかどうかを識別される。これが前者のファイル管理用データの場合には、暗号化・復号化回路 9 が起動せず未処理のままで記憶装置 4 に格納され、一方、後者のファイルデータの場合には、暗号化・復号化回路 9 が起動され、暗号化・復号化キー設定回路 1 0 に設定されたキー情報を用いて暗号化・復号化回路 9 に暗号化演算を行わせ、その暗号化データを記憶装置制御回路 1 2 を介して記憶装置 4 の所定のアドレスに書き込む。以上の判断・指令は、図 2 の破線を経由して C P U 6 が行うものである。

【0 0 2 4】次に、情報記憶媒体 1 a からのデータの読み出しであるが、これは上述の逆の操作を行えばよい。すなわち、ホスト装置 2 が指定した論理アドレス値に基づいて、記憶装置 4 からの読み出しデータがファイル管理用のデータかファイルデータかを識別し、前者には復号化をかけずに後者のみに復号化をかけるように選択的に暗号化・復号化回路 9 を起動させ、暗号化・復号化キー設定回路 1 0 のキー情報を用いて復号化演算を行い、これによりファイルデータ部分のみを復号化してホスト装置 2 に読み出すものである。

【0 0 2 5】以上のように、この実施の形態 1 によれば、暗号化・復号化回路 9 はファイルデータのみに対して暗号化を実行し、既知であるファイル管理用のデータは平文のまま書き込みすることにより、第三者によるこの暗号方式の解読を困難にすることができるのでより高いセキュリティ機能が実現できるという効果が得られる。

【0 0 2 6】実施の形態 2. 図 4 は、この発明の実施の形態 2 によるフラッシュ A T A P C カード等の情報記憶媒体の機能ブロック図である。図において、1 b は情報記憶媒体、3 b は中央制御回路、1 3 はデータ転送バス切り替え回路、S 1, S 2 はスイッチである。その他の構成は、前記実施の形態 1 と同様であるから同一部分には同一符号を付して重複説明を省略する。データ転送バス切り替え回路 1 3 は、暗号化・復号化回路 9 を有効とする場合にはスイッチ S 1, S 2 はそれぞれ P 1, P 3 に接続され、これを無効とする場合にはスイッチ S 1, S 2 はそれぞれ P 2, P 4 に接続されるように作動するものである。

【0 0 2 7】この実施の形態 2 では、拡張コマンドによりファイル毎に暗号化の実行を選択可能とした。このようなファイル単位での暗号化の実行を選択できるようにするために、下記の 3 つの拡張コマンド (1) ~ (3) を定義する。

【0 0 2 8】(1) 暗号化キーロードコマンド
暗号化・復号化のためのキーデータを暗号化・復号化回路 9 にロードするコマンド。

(2) 暗号化付ライトセクタコマンド
ホスト装置 2 よりロードされたキーデータにより暗号化

されたデータを記憶装置 4 に書き込む。

(3) 復号化付リードセクタコマンド
ホスト装置 2 よりロードされたキーデータにより、暗号化されたデータに対し復号化処理を実行し読み出すコマンド。

【0 0 2 9】暗号化付ライトセクタコマンド、または復号化付リードセクタコマンドを発行すると、ホスト装置 2 側のドライバソフトウェアは、その都度暗号化キーコマンドで設定すべき暗号データの入力を要求するように設計されている。したがって、これら暗号化・復号化付ライト・リードコマンド実行時は、そのデータ(ファイル)に固有の暗号化・復号化キーを組み合わせることで入力することにより、通常のリードセクタコマンドでは読み出しができない、セキュリティの高いデータ記憶システムが実現可能となる。

【0 0 3 0】以下、このようにファイル単位での選択的な暗号化・復号化処理を実現する方法について説明する。図 4 において、データ転送バス切り替え回路 1 3 は、ホスト装置 2 の暗号化・復号化付ライト・リードコマンド実行時のみスイッチ S 1, S 2 を P 1, P 3 に接続して暗号化・復号化を有効にし、通常のリードセクタコマンド実行時は暗号化・復号化回路を無効にするようにスイッチ S 1, S 2 を P 2, P 4 に接続して、回路内部のデータ転送ルートの切り替えを実施する。

【0 0 3 1】以上のように、この実施の形態 2 によれば、ホスト装置 2 が上述の拡張コマンド (1) ~ (3) を発行した時のみ暗号化・復号化回路が有効化され、ファイル単位の暗号化が可能となるので、そのファイルデータに固有の暗号化・復号化キーを組み合わせることで入力することにより、通常のリードセクタコマンドでは読み出しができない、セキュリティの高いデータ記憶システムが実現できるという効果が得られる。

【0 0 3 2】実施の形態 3. 図 5 は、この発明の実施の形態 3 によるフラッシュ A T A P C カード等の情報記憶媒体の機能ブロック図である。図において、1 c は情報記憶媒体、3 c は中央制御回路、1 5 はデフォルトキー入力装置であり、その他の構成は、前記実施の形態 1 と同様であるから同一部分には同一符号を付して重複説明を省略する。

【0 0 3 3】次に動作について説明する。P C カード等の情報記憶媒体 1 に格納されるすべてのファイルデータに対して暗号化が実行される。すなわち、通常のリード・リードセクタコマンドの実行時は、暗号化・復号化キー設定回路 1 0 にデフォルトキー入力装置 1 5 より与えられるデフォルトのキーデータにより暗号化・復号化が実行される。また、拡張コマンドである暗号化・復号化付ライト・リードコマンド実行時のみ、組み合わせる暗号化・復号化キーロードコマンドにより設定された固有のキーデータが、暗号化・復号化キー設定回

10

20

30

40

50

路 10 により暗号化・復号化回路 9 に与えられ、暗号化・復号化が実行される。

【0034】以上のように、この実施の形態 3 によれば、拡張コマンド実行時のみ特別のキーデータによる暗号化・復号化回路を実行し、通常のライト・リードセクタコマンド実施時にはデフォルトのキーデータによる暗号化・復号化を実施するように構成したため、暗号化・復号化回路 9 部分の共通化が可能となり、小さな回路規模でファイル単位での選択的な暗号化・復号化が可能な高いセキュリティ機能を有するという効果が得られる。

【0035】また、このデフォルトキー入力装置 15 を上述の実施の形態 2 の場合に適用したものが変形例として考えられ、これは図 6 の情報記憶媒体 1 d に対応するものである。この変形例によれば、前記拡張コマンド実行時のみ特別のキーデータによる暗号化・復号化回路を実行し、通常のライト・リードセクタコマンド実施時にはデフォルトのキーデータによる暗号化・復号化を実施するように構成したことに加えて、ホスト装置 2 が上述の拡張コマンド (1) ~ (3) を発行した時のみデータ転送バス切り替え回路 13 が起動して暗号化・復号化回路が有効化され、ファイル単位の暗号化が可能となるので、そのファイルデータに固有の暗号化・復号化キーを組み合わせることで入力することにより、通常のリードセクタコマンドでは読み出しができないようにも構成することができるので、更にセキュリティの高いデータ記憶システムが実現できるという効果がある。

【0036】実施の形態 4. 前記実施の形態 3 では、拡張コマンドである暗号化・復号化付ライト・リードセクタコマンド実行の度に、組み合わせで発行される暗号化・復号化キーロードコマンドにより、そのファイルに固有のキーデータを設定して暗号化・復号化を実行した。この実施の形態 4 では、暗号化キーロードコマンドによりロードされたキーデータを、新たなキーデータが入力されるまで、またはリセットないし電源オフされるまで有効とし、通常のライト・リードセクタコマンド実行時もこのキーデータによる暗号化・復号化が実行される例を示す。ここでは、デリートキーなるオプションコマンドにより、上述のロード済みのキーデータを消去し、デフォルトのキーデータが有効となる。

【0037】以上のように、この実施の形態 4 によれば、暗号化キーロードコマンドによりロードされたキーデータを、新たなキーデータが入力されるまで、またはリセットないし電源オフされるまで有効としたので、簡易な構成で高いセキュリティを有する効果がある。

【0038】

【発明の効果】以上のように、請求項 1 記載の発明によれば、演算回路がホスト装置からのデータを選択的に暗号化し格納されたデータを復号化するように構成したので、ホスト装置からのデータをその秘密性に依拠して選択的に暗号化・復号化を施すことができ、これにより汎用

性の高い情報記憶媒体であっても格納される貴重な情報に対してセキュリティをかけることができる効果がある。

【0039】請求項 2 記載の発明によれば、演算回路はホスト装置からのデータをファイル単位で選択的に暗号化するように構成したので、ファイル管理用のデータか機密性の高いファイルデータかその種類・用途に応じて暗号化してセキュリティをかけることができる効果がある。

【0040】請求項 3 記載の発明によれば、選択手段がホスト装置からのコマンドに応じて演算回路を有効または無効にするように構成したので、通常のホスト装置のリードコマンドでは読み出しができないように設定することができ、したがってセキュリティの高いデータ記憶システムとすることができる効果がある。

【0041】請求項 4 記載の発明によれば、第 1 演算回路が必要的にデータの書き込み・読み出し双方時にそれぞれ暗号化・復号化し、しかも第 2 演算回路が任意的にデータの書き込み・読み出しの双方時にそれぞれ暗号化・復号化するように構成したので、通常のホスト装置からのコマンドでは第 1 演算回路が動作してデータを暗号化・復号化し、拡張コマンドのときのみ第 2 演算回路が動作して他の暗号化・復号化を行うように設定することができるので、第 1 および第 2 演算回路の共通化が可能となり、小規模回路で選択的な暗号化・復号化が可能なセキュリティ機能を付加できる効果がある。

【0042】請求項 5 記載の発明によれば、第 2 演算回路で行われる暗号化・復号化処理はその回路が更新またはリセットされるまで有効とするように構成したので、簡易なシステムで高いセキュリティを実現する効果がある。

【0043】請求項 6 記載の発明によれば、セクタデータ領域に書き込まれるデータを暗号化し、ファイル管理データに書き込まれるデータには暗号化しないように構成したので、個人情報などの機密性の高いデータに対してより高いセキュリティを持たせることができる効果がある。

【0044】請求項 7 記載の発明によれば、ホスト装置からのコマンドに応じて書き込みデータに暗号化・復号化を実行するように構成したので、通常のホスト装置からのリードセクタコマンドでは読み出しができないセキュリティの高いデータ記憶システムを実現できる効果がある。

【0045】請求項 8 記載の発明によれば、書き込みデータには通常の暗号化・復号化を実行し、特殊キーデータの入力時には他の暗号化・復号化を実行するように構成したので、通常の暗号化・復号化と特殊キーデータの入力時の他の暗号化・復号化を共通の手段で行うことができる。これにより装置規模を縮小できる効果がある。

【0046】請求項 9 記載の発明によれば、特殊キーデ

ータの入力がホスト装置からのコマンドまたは情報記憶媒体に直接行われるように構成したので、ホスト装置および情報記憶媒体の両方面からセキュリティを実行できる効果がある。

【0047】請求項10記載の発明によれば、特殊キーデータの入力が新たなキーデータ入力時または装置リセットないし電源オフまで有効とするように構成したので、簡易なセキュリティソフトウェアの設定で機密保持ができる効果がある。

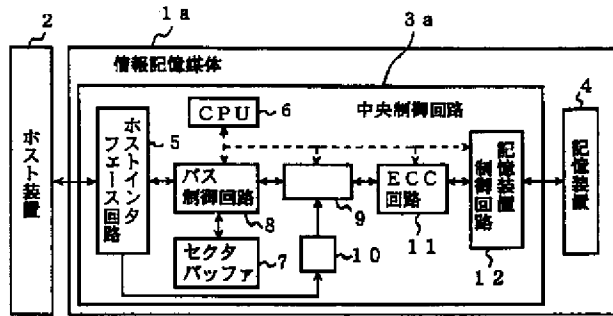
【図面の簡単な説明】

【図1】 この発明の実施の形態1による情報記憶媒体の機能ブロック図である。

【図2】 この発明の実施の形態1による情報記憶媒体のDOSフォーマット後のデータ構成図である。

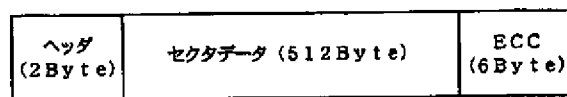
【図3】 この発明の実施の形態1による情報記憶媒体*

【図1】

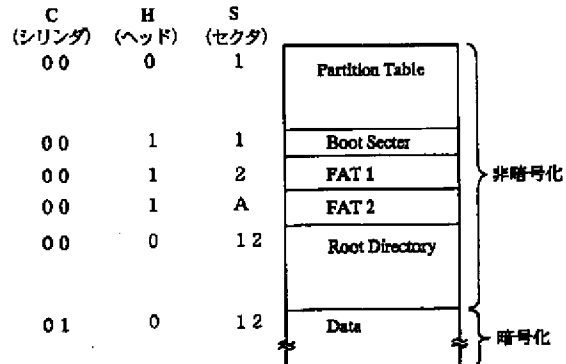


6: CPU (中央処理装置)
9: 暗号化・復号化回路 (演算回路、第1演算回路)
10: 暗号化・復号化キー設定回路 (演算回路、第2演算回路)

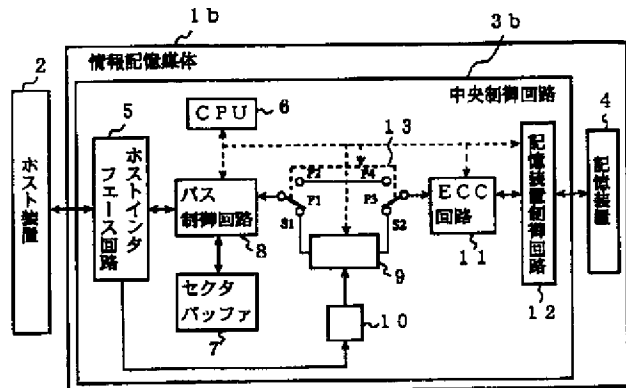
【図3】



【図2】



【図4】



*のデータ構成図である。

【図4】 この発明の実施の形態2による情報記憶媒体の機能ブロック図である。

【図5】 この発明の実施の形態3による情報記憶媒体の機能ブロック図である。

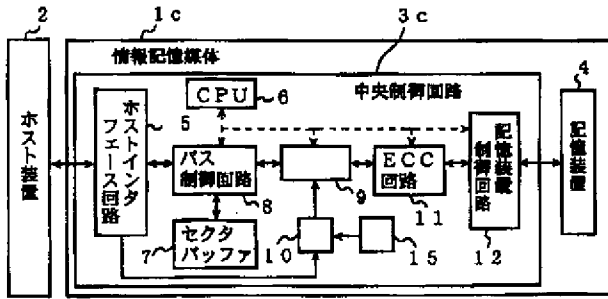
【図6】 この発明の実施の形態3の変形例による情報記憶媒体の機能ブロック図である。

【図7】 従来の情報記憶媒体の機能ブロック図である。

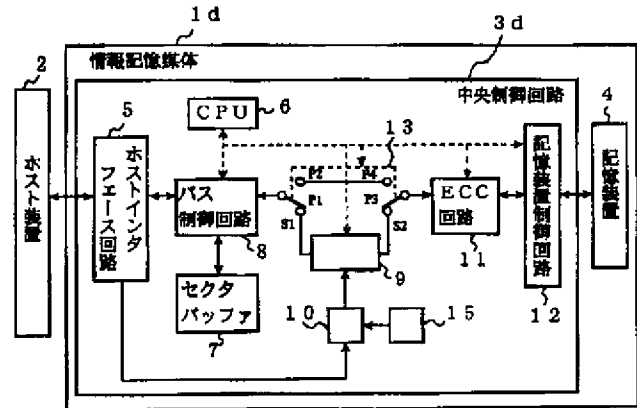
10 【符号の説明】

1a~1e 情報記憶媒体、2 ホスト装置、4 記憶装置、6 CPU (中央処理装置)、9 暗号化・復号化回路 (演算回路、第1演算回路)、10 暗号化・復号化キー設定回路 (演算回路、第2演算回路)。

【図5】



【図6】



【図7】

